天翼云·密评专区

用户使用指南

天翼云科技有限公司

目录

1 产品简介

1.1 产品定义

商用密码应用安全性评估是指在采用商用密码算法、密码技术、密码产品和密码服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性进行评估。《中华人民共和国密码法》在 2020 年 1 月 1 日施行，《密码法》第二十七条明确规定了“法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估”。

天翼云密评专区产品是以商用密码技术、产品、服务为基础，使用具备商用密码产品认证证书的云密码机在云上构建密码资源池，为云上应用提供通过密评所需的各类密码服务，包括密钥管理服务、数据加解密服务、身份认证服务、签名验签服务、协同签名服务、时间戳服务等。

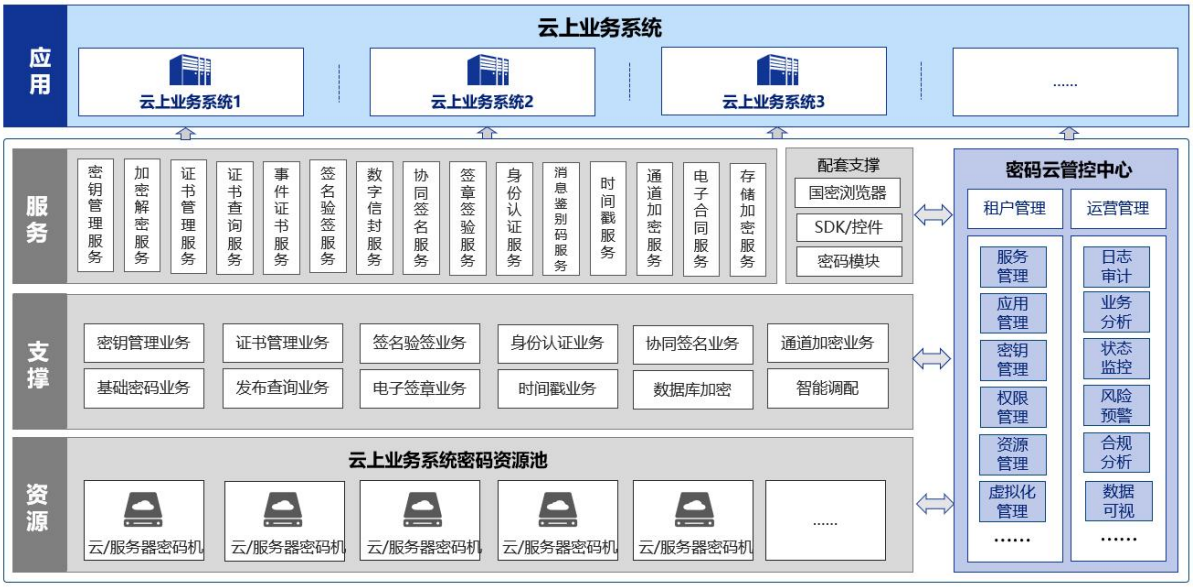
密评专区由资源层、支撑层、服务层以及云管控中心四部分组成：

资源层：通过云密码机组建密码资源池，提供密码算力。

支撑层：提供密钥管理管理能力及各类密码服务的支撑能力。

服务层：为云上业务系统提供密评所需要的通用和典型密码服务。

管控中心：提供对租户、应用的管理能力以及业务的统计分析、监控预警能力。



1.2 产品优势

1.2.1 满足密评合规

密评专区使用的软硬件产品都具备商用密码产品认证证书，为应用系统提供通过密评所需的基于商用密码的合规密码服务，应用系统通过密码应用改造最终通过密评。

1.2.2 全场景密码服务

密评专区提供全场景密码服务能力，不仅提供加解密、身份认证、签名验签等通用密码服务，也可提供电子签章、时间戳、协同签名等典型密码服务，满足应用系统的各类密码服务需求。

1.2.3 应用改造便捷

密评专区提供统一标准的密码服务接口，应用改造简单快捷，具备完备的应用接入指南并提供及时、优质的技术支持服务。

1.2.4 一站式专业服务

一对一专属项目经理，7*24h 技术支持，31 省本地化的销售网络体系，提供“家门口”的精细化客户服务。

1.3 产品功能

天翼云密评专区产品具有以下功能。

1.3.1 全场景密码服务能力

密评专区提供全场景密码服务能力，不仅提供加解密、身份认证、签名验签等通用密码服务，也提供电子签章、时间戳、协同签名等典型密码服务，满足应用系统的各类密码服务需求。

1.3.2 统一服务接口，应用改造便捷

密评专区提供统一标准的密码服务接口，应用改造简单快捷，具备完备的应用接入指南并提供及时、优质的技术支持服务。

1.3.3 按需分配和弹性扩容能力

✓ 采用容器虚拟化技术，实现服务实例的按需分配。

✓ 使用云密码机构建云密码资源池，密码计算能力支持弹性扩展。

1.3.4 满足密评合规

密评专区使用的软硬件产品都具备商用密码产品认证证书，为应用系统提供通过密评所需的基于商用密码的合规密码服务，应用系统通过密码应用改造最终通过密评。

1.4 产品特性

天翼云密评专区产品具有以下特性。

1.4.1 加解密服务

为应用系统提供重要数据的加密和解密服务，满足密评中对重要数据传输和存储的机密性要求。

1.4.2 身份认证服务

为应用系统提供对登录用户的基于国密数字证书身份认证服务，保证应用系统用户身份的真实性，满足密评中对用户身份真实性鉴别的要求。

1.4.3 签名验签服务

为应用系统提供重要数据的签名和验签服务，满足密评中对重要数据传输和存储的完整性要求以及操作的不可否认性要求。

1.4.4 密钥管理服务

为应用系统提供集中的密钥全生命周期管理服务，满足密评中对密钥管理的安全性要求。

1.4.5 杂凑密码服务

为应用系统提供杂凑密码运算服务，满足密评中对重要数据传输和存储的完整性要求。

1.4.6 数字证书服务

为用户、应用或设备提供数字证书的签发、更新、注销等全生命周期的管理，为身份鉴别提供数字证书支撑服务。

1.4.7 SSL 加密服务

提供网络通信通道的加密服务，满足密评中对网络和通信安全层面的数据传输机密性和完整性要求。

1.4.8 电子签章服务

为应用系统提供电子签章服务，电子签章以数字证书为基础，将数字签名、印章图片以及被签章对象进行结合，通过签章形式，满足不可否认性要求。

1.4.9 协同签名服务

配合移动端密码模块为应用系统移动端提供协同密码服务，满足移动端的密码应用合规性要求。

1.4.10 时间戳服务

为应用系统提供用于证明原发数据的产生时间，满足时间不可否认性的要求。

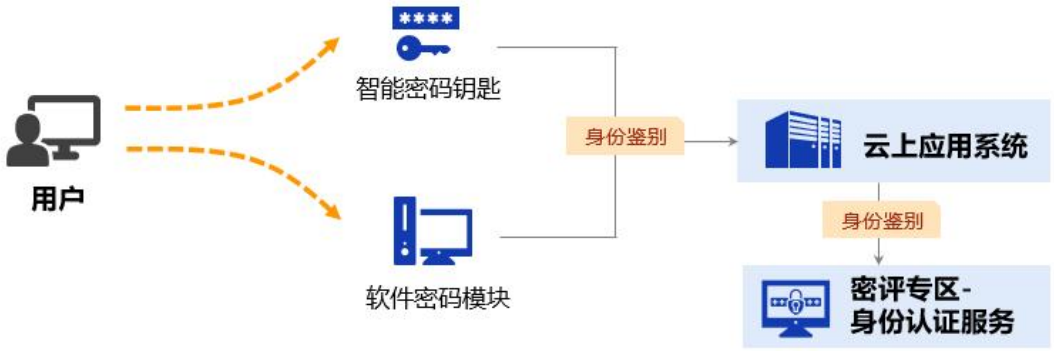
1.5 应用场景

1.5.1 登录用户身份鉴别

- 场景说明：密评中应用与数据安全层面的登录用户身份鉴别要求，应用系统的登录用户使用基于国密数字证书的身份认证服务，满足用户身份真实性要求。
- 解决的问题
  - ✓ 【登录用户身份真实性】为登录用户签发数字证书，存储在智能密码钥匙或软件密码模块中，用户登录应用系统前使用自己的证书完成登录信息提交，云上应用系统调用密评专区的身份认证服务，完成登录用户的

身份鉴别，通过基于国密算法的数字证书身份认证机制，保障登录用户的身份真实性。

- 使用场景图



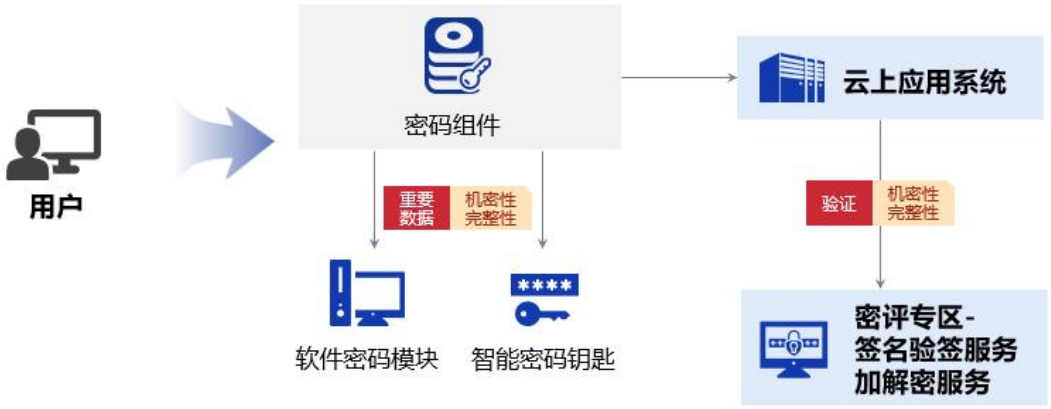
1.5.2 重要数据安全传输

- 场景说明：密评中应用与数据安全层面的重要数据传输机密性和完整性要求，应用系统的重要数据在传输前调用密评专区的数据加解服务、签名服务对数据进行机密性和完整性保护，传输完成后进行解密和验签，保障数据传输过程中的安全性。

- 解决的问题

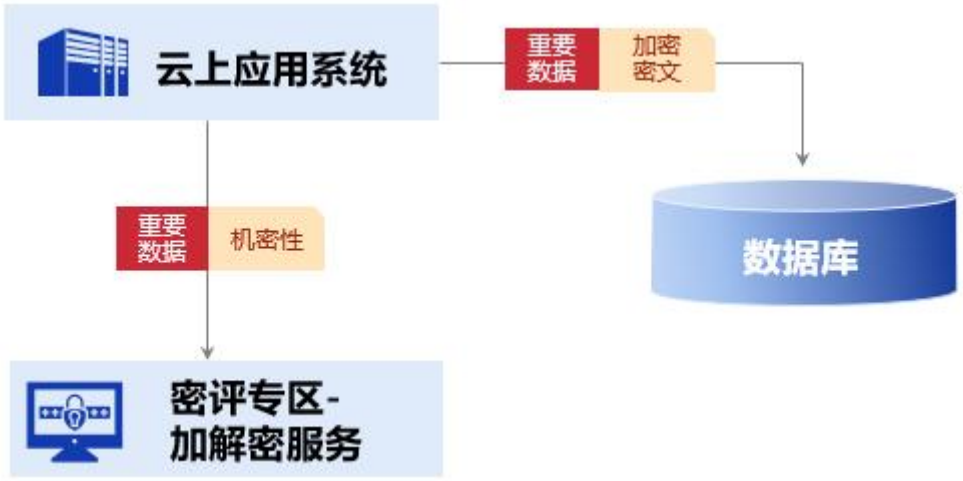
  - ✓ 【传输机密性】重要数据传输前，云上应用系统调用密评专区的加密服务（终端调用智能密码钥匙或软件密码模块），对数据进行加密后再传输，保障重要数据传输机密性。
  - ✓ 【传输完整性】重要数据传输前，云上应用系统调用密评专区的签名服务（终端调用智能密码钥匙或软件密码模块），对数据进行签名后再传输，保障重要数据传输完整性。

- 使用场景图



1.5.3 重要数据加密存储

- 场景说明：密评中应用与数据安全层面的重要数据存储机密性要求，应用系统的重要数据存储到数据库时需要进行加密保存，应用系统调用密评专区的数据加密服务进行数据加密，把加密后的密文保存到数据库，满足数据存储机密性要求。
- 解决的问题
  - ✓ 【重要数据存储机密性】云上应用系统调用密评专区的加解密服务，对重要数据进行加密后存储到数据库，完成重要数据的机密性保护，数据库中的数据为加密后的密文，防止重要数据在存储过程中被窃取的风险。
- 使用场景图



1.6 产品规格

密评专区包括密码支撑服务、密码支撑打包服务、终端密码服务三种规格，其中，密码支撑服务分为基础版和高级版。

规格名称	名称	产品计费模式（包年/按量）	购买说明
密码支撑服务	基础版	包年	1、适用于使用密码服务的应用数量较少的租户（5 个应用以内）。 2、根据需要使用密码服务的应用数量购买。 3、如果有电子签章/时间戳/协同签名的服务需要选择高级版，不需要以上 3 个服务的选择基础版，如果不能确定需要哪些服务的建议选择高级版。
	高级版	包年	

规格名称	名称	产品计费模式（包年/按量）	购买说明
密码支撑打包服务	10 应用	包年	1、可以简单这样理解：密码服务是零售、密码打包服务就是批发。 2、适用于使用密码服务的应用数量较多的租户（5 个应用以上）。 3、折合单应用密码服务单价更低，根据实际使用密码服务的数量选择合适的规格。
	20 应用	包年	
	50 应用	包年	
	100 应用	包年	
	200 应用（上限）	包年	
终端密码服务	VPN 并发数	按量包年	VPN 并发数根据租户实际用户数量按 10：1 购买（比如租户共 1000 个人使用 VPN 服务，则购买 100 的并发数），一个租户购买一年购买一次就可以，不需要每个应用都购买。
	智能密码钥匙	按量	智能密码钥匙根据 PC 端使用数字证书的人员数量购买。
	软件密码模块	按量	软件密码模块根据移动端使用密码服务的数量购买。

1.7 术语解释

密评：全称“商用密码应用安全性评估”，指在采用商用密码算法、密码技术、密码产品和密码服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性进行评估。

密码：《中华人民共和国密码法 》中所述的密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。

商用密码：国内密码分为核心密码、普通密码、商用密码三类，其中核心密码、普通密码是用于保护国家秘密信息，商用密码保护非涉密信息。商用密码技术和产品是指基于商用密码对不涉及国家秘密内容的信息进行加密保护或安全认证所使用的技术和产品。

国密算法：国家密码管理局基于 ECC 椭圆曲线加密算法开发的新一代中国自主控制的加密算法，是目前国家密码管理局在商业密码领域强制实施的标准。

数字签名：采用 PKI 技术，先对原文信息进行摘要（Hash），然后通过私钥进行签名处理，生成签名信息，签名信息只有私钥才能产生，签名过程不可逆,通过数字签名，可以保证明文数据的完整性和不可抵赖性。

数据完整性：表明数据没有遭受以非授权方式所作的篡改或破坏。

不可抵赖性：又称不可否认性，是指对行为的确认，确定行为必须是某人或某机构所为，不能否认，数字签名通过非对称密码技术和 PKI 管理体制保证不可抵赖实现。

X.509 证书标准：国际电话与电报咨询委员会(CCITT)规定的一种行业标准。在这个标准中提供了一个数字证书的标准格式，规定数字证书必须包含的一些信息：如版本号、序列号、签名算法、有效期限等。

2 计费说明

2.1 计费项

规格名称	名称	产品计费模式（包年/按量）	商品目录价
密码支撑服务	基础版	包年	200,000 元/年
	高级版	包年	320,000 元/年
密码支撑打包服务	10 应用	包年	1,400,000 元/年
	20 应用	包年	2,100,000 元/年
	50 应用	包年	4,000,000 元/年
	100 应用	包年	5,800,000 元/年
	200 应用（上限）	包年	10,000,000 元/年
终端密码服务	VPN 并发数	包年	300 元/个
	智能密码钥匙	按量	80 元/个
	软件密码模块	按量	50 元/个

2.2 订购、续订、退订

订购操作需要客户联系专属客户经理，如果没有专属客户经理，可拨打天翼云客服电话 4008-109-889 咨询。

2.2.1 订购

用户在购买该产品之前咨询客户经理，待需求明确后客户经理根据业务需求选择对应的产品规格，通过提交业务需求单方式下单购买，可以通过包周期计费购买，业务数量多打包购买更合适。

2.2.2 续订

在“资产实例列表”中查看您已经订购的资源，点击“详情”选择续订，如下图所示：

2.2.3 退订

在“资产实例列表”中查看您已经订购的资源，点击“详情”选择退订，如下图所示：

2.3 增值/定制内容申请

如果您有增值/定制的需求，您可以联系客户经理或天翼云客服，提交您的需求。也可以进入官网以工单的形式提交您的需求。

热线电话：4008-109-889

提交工单：https://www.ctyun.cn/h5/wsc/worksheet/submit

3 常见问题

3.1 技术类

3.1.1 为什么要做密评?

开展密评，是为了解决商用密码应用中存在的突出问题，为网络和信息系统的安全提供科学评价方法，逐步规范商用密码的使用和管理。从根本上改变商用密码应用不广泛、不规范、不安全的现状，确保商用密码在网络和信息系统中有效使用，切实构建起坚实可靠的网络安全密码屏障。

《密码法》第二十七条：法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。

《商用密码管理条例》第六章第三十八条：法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，自行或者委托商用密码检测机构开展商用密码应用安全性评估。

《商用密码应用安全性评估管理办法（试行）》第一章第三条：“涉及国家安全和社会公共利益的重要领域网络和 信息系统的建设、使用、管理单位应当健全密码保障体系，实施商用密码应用安全性评 估”。重要领域网络和信息系统包括：基础信息网络、涉及国计民生和基础信息资源的 重要信息系统、重要工业控制系统、面向社会服务的政务信息系统，以及关键信息基础 设施、网络安全等级保护第三级及以上信息系统。

3.1.2 密评整体流程?

密评整体流程共包括 4 个阶段，分别为编写密码应用方案、密码应用方案评估、系统建设/改造、密码应用安全性评估。

编写密码应用方案：客户首先自行或委托密评机构按照密评标准对系统进行差距分析，根据差距分析结果结合系统实际情况设计密码应用方案，密码应用方案应包括系统现状及存在的风险、系统涵盖的重要数据、密码应用需求、方案设计以及使用的密码技术、管理制度、应急方案以及实施方案等。

密码应用方案评估：密码应用方案编写完成后，可委托密码专家或密评机构对密码应用方案进行评审，若委托密码专家对方案评审则出具专家评审意见，若委托密评机构评审，则出具密码应用方案评估报告。

系统建设/改造：密码应用方案通过评审后，系统集成单位按照通过评审的方案对系统进行建设或改造。

密码应用安全性评估：系统建设/改造完成后，被测单位委托密评机构对系统进行测评，密评机构按照 GB/T 39786 标准测评并出具差距分析报告，客户根据差

距分析结果进行整改并申请复测，最终出具符合要求的商用密码应用安全性评估报告。

3.1.3 密评专区的防护功能是否就能满足密评合规需求?

密评专区可满足密评二级、三级的安全技术合规要求，密评第一级~第四级密码应用基本要求见下表。

对于“可”的条款，由信息系统责任单位自行决定是否纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照相应的测评指标要求进行测评和结果判定；否则，该测评指标为“不适用”。

对于“宜”的条款，密评人员根据信息系统的密码应用方案和方案评审意见决定是否纳入标准符合性测评范围；若信息系统没有通过评估的密码应用方案或密码应用方案未做明确说明，则“宜”的条款默认纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照测评指标要求进行测评和结果判定。否则，密评人员应根据信息系统的密码应用方案和方案评审意见，在测评中进一步核实密码应用方案中所描述的风险控制措施使用条件在实际的信息系统中是否被满足，且信

息系统的实施情况与所描述的风险控制措施是否一致，若满足使用条件，该测评指标为“不适用”，并在密码应用安全性评估报告中体现核实过程和结果；若不满足使用条件，则应按照测评指标要求进行测评和结果判定。

对于“应”的条款，密评人员应按照测评指标要求进行测评和结果判定；若根据信息系统的密码应用方案和方案评审意见，判定信息系统确无与某项或某些项测评指标相关的密码应用需求，则相应测评指标为“不适用”。

表 A.1　第一级～第四级密码应用基本要求汇总列表

指标体系			第一级	第二级	第三级	第四级
技术要求	物理和环境安全	身份鉴别	可	宜	宜	应
		电子门禁记录数据存储完整性	可	可	宜	应
		视频监控记录数据存储完整性	—	—	宜	应
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
	网络和通信安全	身份鉴别	可	宜	应	应
		通信数据完整性	可	可	宜	应
		通信过程中重要数据的机密性	可	宜	应	应
		网络边界访问控制信息的完整性	可	可	宜	应
		安全接入认证	—	—	可	宜
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
	设备和计算安全	身份鉴别	可	宜	应	应
		远程管理通道安全	—	—	应	应
		系统资源访问控制信息完整性	可	可	宜	应
		重要信息资源安全标记完整性	—	—	宜	应
		日志记录完整性	可	可	宜	应
		重要可执行程序完整性、重要可执行程序来源真实性	—	—	宜	应
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
	应用和数据安全	身份鉴别	可	宜	应	应
		访问控制信息完整性	可	可	宜	应
		重要信息资源安全标记完整性	—	—	宜	应
		重要数据传输机密性	可	宜	应	应
		重要数据存储机密性	可	宜	应	应
		重要数据传输完整性	可	宜	宜	应
		重要数据存储完整性	可	宜	宜	应
		不可否认性	—	—	宜	应
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上

指标体系			第一级	第二级	第三级	第四级
管理要求	管理制度	具备密码应用安全管理制度	应	应	应	应
		密钥管理规则	应	应	应	应
		建立操作规程	—	应	应	应
		定期修订安全管理制度	—	—	应	应
		明确管理制度发布流程	—	—	应	应
		制度执行过程记录留存	—	—	应	应
	人员管理	了解并遵守密码相关法律法规和密码管理制度	应	应	应	应
		建立密码应用岗位责任制度	—	应	应	应
		建立上岗人员培训制度	—	应	应	应
		定期进行安全岗位人员考核	—	—	应	应
		建立关键岗位人员保密制度和调离制度	应	应	应	应
	建设运行	制定密码应用方案	应	应	应	应
		制定密钥安全管理策略	应	应	应	应
		制定实施方案	应	应	应	应
		投入运行前进行密码应用安全性评估	可	宜	应	应
		定期开展密码应用安全性评估及攻防对抗演习	—	—	应	应
	应急处置	应急策略	可	应	应	应
		事件处置	—	—	应	应
		向有关主管部门上报处置情况	—	—	应	应

3.2 使用说明类

3.2.1 如何确定被测信息系统密码应用等级?

GB/T 39786-2021 中的密码应用等级一般由网络安全等级保护的级别确定。信息系统根据 GB/T 22240-2020《信息安全技术网络安全等级保护定级指南》确定等级保护级别时，同步对应确定密码应用等级，即等保定级为第一级的网络与信息系统应遵循 GB/T 39786-2021 第一级密码应用基本要求，等保定级为第二

级的网络与信息系统应遵循 GB/T 39786-2021 第二级密码应用基本要求，以此类推。对于未完成网络安全等级保护定级的重要信息系统，其密码应用等级至少为第三级。因此在进行密码测评时，建议至少先完成等保的定级备案。

3.2.2 资源池没过密评，客户能部署密评专区过密评，拿到测评报告吗？

云平台是否过密评不会直接影响租户侧的密评结果，若平台侧已经通过密评，那么云上租户在进行商用密码应用安全性评估时可复用平台侧的部分结果，如云平台已经进行了测评且拿到符合要求的密评报告，那么云上租户在进行测评时可复用物理和环境安全（即机房）的测评结果，反之，若平台侧没有通过密评，那么云上租户在进行密码测评时则不能复用平台侧的测评结果，需要按照密评标准 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》逐条测评。

3.2.3 购买了密评专区是否还需要购买密码测评服务？

需要，密评专区主要为客户提供密码改造服务，即根据客户的业务需求提供加解密、签名验签、SSL 加密服务等接口，协助客户按照密评标准满足身份鉴别、通道加密、重要数据存储等指标，需要由客户和云公司共同完成，而密码测评指的是系统建设/改造完成后委托密评机构按照密评标准 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》分别从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行和应急处置

等多个维度对系统进行测评，由测评机构、客户和云公司共同完成，目前全国共有 48 家密评机构可进行全国系统的测评。

3.2.4 应用系统是否涉及代码改造?

客户在购买了密评专区后还需要对应用系统进行代码改造才能满足业务系统的密码需求，客户通过业务系统实际需求调用密评专区对应的服务，如身份鉴别不满足需求，则需要调用身份认证服务对应的接口，如未对重要业务数据进行安全存储，则根据实际需求，若重要数据需要进行防泄漏（机密性）保护，则调用加解密服务接口以保证重要业务数据的存储机密性，若重要数据需要进行防篡改（完整性）保护，则第哦啊用签名验签及服务接口保证重要数据的存储完整性。密评专区可提供的服务见下表。

密码服务	服务说明
加解密服务	为应用系统提供重要数据的加密和解密服务，满足密评中对重要数据传输和存储的机密性要求。
身份认证服务	为应用系统提供对登录用户的基于国密数字证书的身份认证服务，保证应用系统用户身份的真实性，满足密评中对用户身份真实性鉴别的要求。
签名验签服务	为应用系统提供重要数据的签名和验签服务，满足密评中对重要数据传输和存储的完整性要求以及操作的不可否认性要求。
密钥管理服务	为应用系统提供集中的密钥全生命周期管理服务，满足密评中对密钥

密码服务	服务说明
	管理的安全性要求。
杂凑密码服务	为应用系统提供杂凑密码运算服务，满足密评中对重要数据传输和存储的完整性要求。
数字证书服务	为用户、应用或设备提供数字证书的签发、更新、注销等全生命周期的管理，为身份鉴别提供数字证书支撑服务。
SSL 加密服务	提供网络通信通道的加密服务，满足密评中对网络和通信安全层面的数据传输机密性和完整性要求。
电子签章服务	为应用系统提供电子签章服务，电子签章以数字证书为基础，将数字签名、印章图片以及被签章对象进行结合，通过签章形式，满足不可否认性要求。
协同签名服务	配合移动端密码模块为应用系统移动端提供协同密码服务，满足移动端的密码应用合规性要求。
时间戳服务	为应用系统提供用于证明原发数据的产生时间，满足时间不可否认性的要求。

3.3 计费类

3.3.1 密评专区有哪些计费项?

密评专区共两大类计费项，分别为密码支撑服务（密码支撑打包服务）费和终端密码服务费。其中密码支撑服务（密码支撑打包服务）根据应用系统数量按年计费，终端密码服务根据用户终端数量按量购买。

规格名称	名称	产品计费模式（包年/按量）	购买说明
密码支撑服务	基础版	包年	1、适用于使用密码服务的应用数量较少的租户（5 个应用以内）。 2、根据需要使用密码服务的应用数量购买。 3、如果有电子签章/时间戳/协同签的服务需要选择高级版，不需要以上 3 个服务的选择基础版，如果不能确定需要哪些服务的，建议选择高级版。
	高级版	包年	
密码支撑打包服务	10 应用	包年	1、可以简单的这样理解：密码服务是零售、密码打包服务就是批发。 2、适用于使用密码服务的应用数量较多的租户（5 个应用以上）。
	20 应用	包年	
	50 应用	包年	
	100 应用	包年	

	200 应用（上限）	包年	3、折合单应用密码服务单价更低，根据实际使用密码服务的数量选择合适的规格。
终端密码服务	VPN 并发数	按量包年	VPN 并发数根据租户实际用户数量按 10:1 购买（比如租户共 1000 个人使用 VPN 服务，则购买 100 的并发数），一个租户购买一年，购买一次就可以，不需要每个应用都购买。
	智能密码钥匙	按量	智能密码钥匙根据 PC 端使用数字证书的人员数量购买。
	软件密码模块	按量	软件密码模块根据移动端使用密码服务的数量购买。

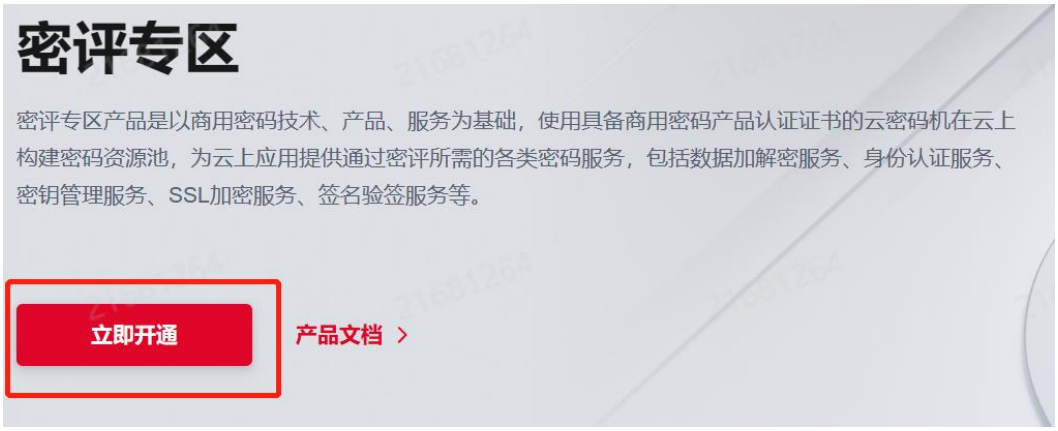
3.3.2 该产品如何购买?

客户在自行或委托密评机构对系统进行差距分析后，根据差距分析结果结合系统实际情况分析密码需求，根据密码需求结合密评专区各规格提供的服务选择合适的产品规格（见下表），若系统数量大于 5 个，选择密码密码打包服务，若系统数量小于 5 个，则根据系统的密码需求，如果涉及时间戳服务、电子签章服务或协同签名服务，则选择密码服务高级版，反之，选择密码服务基础版。

密码服务基础版	密码服务高级版	密码打包服务

密码服务基础版	密码服务高级版	密码打包服务
加解密服务	加解密服务	加解密服务
签名验签服务	签名验签服务	签名验签服务
杂凑密码服务	杂凑密码服务	杂凑密码服务
密钥管理服务	密钥管理服务	密钥管理服务
数字证书服务	数字证书服务	数字证书服务
SSL 加密服务	SSL 加密服务	SSL 加密服务
身份认证服务	身份认证服务	身份认证服务
	时间戳服务	时间戳服务
	电子签章服务	电子签章服务
	协同签名服务	协同签名服务

选择完对应的产品规格后，点击“立即开通”，在业务需求单中填写业务需求。



3.3.3 密评专区产品包含哪些计费模式，客户该如何选择?

密评专区包括密码支撑服务、密码支撑打包服务和终端密码服务三种规格，密码支撑服务和密码支撑打包服务支持包年计费方式，终端密码服务支持按量计费方式。

终端密码服务为必选项，密码支撑服务和密码支撑打包服务二选一。可以简单的理解为密码服务为零售、密码打包服务就是批发，密码支撑服务适用于应用数量较少的客户，建议 5 个以下的应用系统过密评按照应用系统数量购买密码支撑服务即可，若需要使用密码服务的应用数量较多（5 个以上），则选择密码支撑打包服务。

3.3.4 密码支撑服务基础版和高级版的区别?

高级版比基础版多了电子签章、时间戳和协同签名 3 个服务，如果应用系统不涉及电子签章需求或对时效性要求不高，则选择基础版即可。电子签章服务和时间

戳服务都为了满足密码中不可否认性的需求，在可能涉及法律责任认定的应用中，需要提供数据原发证据和接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性，如公文审批、金额交易等重要操作，协同签名主要满足使用移动端登录用户的身份鉴别需求。

3.3.5 终端密码服务如何购买?

终端密码服务包括 VPN 并发数、智能密码钥匙和软件密码模块 3 种。智能密码钥匙的购买数量根据 PC 端使用数字证书登录的用户来定，软件密码模块根据移动端使用密码的用户数量来定，VPN 并发数根据租户实际用户数量按 10:1 购买。比如某应用系统有 325 个用户，其中 240 个用户需要通过 PC 端登录业务系统进行身份鉴别，85 个用户通过移动 APP 登录，那么需要购买智能密码钥匙的数量为 240 个，需要购买软件密码模块的数量为 85 个，VPN 并发数为 325/10=32.5，因一 VPN 并发数按照整数购买，所以 VPN 并发数最少购买 33 个，以上购买量均按系统实际需求购买，若考虑后期仍有新用户，可在目前基础上进行增加。

3.3.6 本产品是否支持试用?

因本产品涉及对应用系统的代码改造，**本产品不支持试用**，建议在购买之前先对系统完成差距分析，根据差距分析结果及业务系统的实际密码需求选择对应的产品规格再购买。